REMARKS

This is a full and timely response to the outstanding final Office Action mailed October 12, 2005. Reconsideration and allowance of the application and pending claims are respectfully requested.

I. Allowable Subject Matter

Applicant appreciates the Examiner's indication that claims 26-30 are allowable. In that it is believed that every rejection has been overcome, it is respectfully submitted that each of the claims that remains in the case is presently in condition for allowance.

II. Claim Rejections - 35 U.S.C. § 102(e)

Claims 1-25 have been rejected under 35 U.S.C. § 102(e) as being anticipated by Strahm et al. ("Strahm," U.S. Pub. No. 2002/0104020). Applicant respectfully traverses this rejection.

It is axiomatic that "[a]nticipation requires the disclosure in a single prior art reference of each element of the claim under consideration." *W. L. Gore & Associates, Inc. v. Garlock, Inc.*, 721 F.2d 1540, 1554, 220 USPQ 303, 313 (Fed. Cir. 1983). Therefore, every claimed feature of the claimed invention must be represented in the applied reference to constitute a proper rejection under 35 U.S.C. § 102(e).

In the present case, not every feature of the claimed invention is represented in the Strahm reference. Applicant discusses the Strahm reference and Applicant's claims in the following.

A. The Strahm Reference

Strahm discloses a system for processing Internet protocol security (IPSec) traffic. Strahm, Application Title. As is described by Strahm, packets sent from a source (i.e., control element 206) arrive at a classifying forwarding element (CFE) 202, which attempts to classify the packet. Strahm, paragraph 0029. As is described by Strahm, the CFE 202 classifies the packet ***by accessing the packet's contents***. Strahm, paragraph 0029.

Once the packet is classified, the CFE 202 forwards the packet to any one of multiple decrypting forwarding elements (DFEs) 204. Strahm, paragraph 0030. As is described by Strahm, the decision as to which DFE to route the packet to is unimportant. Specifically, Strahm states:

> The CFE 202 can use any selection technique to choose which DFE 204a-204c receives the packet 210. For example, the CFE 202 could implement a load balancing technique that distributes packets to the DFEs 204a-204c based on resource availability of the DFEs 204a-204c and/or the servers 214a-214c associated with the DFEs 204a-204c. In another example, the CFE 202 could implement a fixed scheme that distributed packets to the DFEs 204a-204c based on a fixed rotating order or based on a round robin scheme.
> [Strahm, paragraph 0030]

Although Strahm states that the packet may include a security association (SA), Strahm says ***nothing*** about deciding where to route a packet to based upon a security association of the packet.

B. Applicant's Claims

1. Claims 1-14

Applicant's claim 1, as amended, provides as follows (emphasis added):

> 1. An apparatus for performing network routing, the apparatus comprising:
>
> authentication logic configured to receive packets sent from a source agent to an endpoint of a tunnel and to determine whether a security association of a packet received corresponds to said source agent, the tunnel being configured by said source agent in accordance with a network protocol;
>
> decision logic ***configured to make a routing decision for each authenticated packet at least in part without regard to contents of a payload of the packet, the routing decision being based on the security association of the authenticated packet***; and
>
> routing logic configured to select a routing destination for each authenticated packet and to route the authenticated packet to the selected routing destination, the routing destination selection being based at least partially on said routing decision.

In the Office Action, it is stated that Strahm teaches decision logic configured to make a routing decision for each authenticated packet that is constrained based on the security association of the authenticated packet. Applicant respectfully disagrees.

Strahm describes his disclosed method for processing packets in detail in paragraphs 0029 to 0036. As is explained in those paragraphs, and as is summarized above by Applicant, a packet 210 arrives at the classifying forwarding element (CFE) 202, which has the responsibility of "classifying" the packet. Strahm, paragraph 0029.

The CFE accesses the packet's contents and "classifies" the packet ***based upon the information contained in the packet's contents***. Strahm, paragraph 0029. After the classifying is completed, the CFE forwards the classified packet to one of several decrypting forwarding elements (DFEs). Strahm, paragraph 0030. In view of this, Strahm's system clearly does not make a routing decision "without regard to contents of a payload of the packet" or make a routing decision that is "based on the security association of the authenticated packet" as are required by claim 1. Claim 1 and its dependents are allowable over Strahm for at least this reason.

As a further point, Applicant notes that it cannot simply be presumed that Strahm uses the security association to make the routing decision. Indeed, if any presumption is to be made, the ***opposite*** should be presumed. Specifically, as is described in Applicant's original disclosure, the security association is normally not used to make a routing decision according to IPSec protocol. As is stated in that disclosure:

> . . . each IPSec packet will include a destination IP address, an ESP header, and a payload. The payload includes, among other information, an internal destination address and data, both of which may be encrypted. As stated above, if the payload packet is successfully authenticated at the destination endpoint, the decrypted internal destination address is normally used by the endpoint device to determine the destination to which the decrypted packet is to be routed within the private network.
> [Applicant's specification, page 15, lines 14-19]

Moreover, as is also described in Applicant's specification, routing based upon an internal destination address included in the packet payload is even dictated by the IPSec

protocol, which is used in Strahm's system. See Applicant's specification, page 16, lines 11-17.

In the outstanding Office Action, the Examiner argues that Strahm discloses that the CFE 202 "classifies" packets based on the packet's security association, and cites paragraph 0009 of the Strahm disclosure. That paragraph provides as follows:

> [0009] Operations of the CFE 202 include classifying the traffic it receives from the network 212 for transmission to a destination, such as a server 214a, 214b, or 214c, or from one of the servers 214a-214c for transmission to the network 212. This classifying can involve adding a header/trailer, load balancing, intrusion detection, firewalling, and other similar route optimization and security tasks. The CFE 202 classifies the traffic based on parameters sent to it by the CE 206. The parameters can include IPsec Security Parameter Index (SPI) information.
> [Strahm, paragraph 0009]

As can be appreciated from the above, paragraph 0009 of the Strahm disclosure is silent as to classifying packets *based on the packet's security association.*

Later in the Office Action, it is argued that using an address in a security association to make a routing decision is "known in the art." Applicant notes that no support for this conclusion is provided in the Office Action. Accordingly, it appears as though the Examiner is taking Official Notice of the concept of routing packets based upon an address contained in a security association. The Manual of Patent Examining Procedure (MPEP) defines the standard for taking Official Notice. As provided in MPEP § 2144.03:

> Official notice without documentary evidence to support an examiner's conclusion is permissible only in some circumstances. While "official notice" may be relied on, these circumstances should be rare when an application is under final rejection or action under 37 CFR 1.113. Official notice unsupported by documentary evidence should only be taken by the examiner where the facts asserted to be well-known, or to be common knowledge in the art are capable of instant and unquestionable demonstration as being well-known. As noted by the court in *In re Ahlert*, 424, F.2d 1088, 1091, 165 USPQ 418, 420 (CCPA 1970), the notice of facts beyond the record which may be taken by the examiner must be "capable of such instant and unquestionable demonstration as to defy dispute" (citing *In re Knapp Monarch Co.*, 296 F.2d 230, 132 USPQ 6 (CCPA 1961)).

As provided in MPEP § 2144.03 (emphasis added):

> If applicant adequately traverses the examiner's assertion of official notice, ***the examiner must provide documentary evidence in the next Office action*** if the rejection is to be maintained. See 37 CFR 1.104(c)(2).

In the instant case, Applicant respectfully submits that routing packets based upon an address contained in a security association is not so known so as to be capable of "instant and unquestionable demonstration." Indeed, as is described above, the practice dictated by IPSec is to route based upon information contained in the packet payload, ***not*** the security association. Accordingly, Applicant traverses the Examiner's use of Official

Notice. Because of this traversal, the Examiner ***must*** support his finding with evidence, or withdraw the Official Notice determination as per MPEP § 2144.03.

2. Claims 15-23

Applicant's claim 15 provides as follows (emphasis added):

> 15. A method for performing network routing, the method comprising:
>
> authenticating received packets sent from a source agent to an endpoint of a tunnel by determining whether a security association of a received packet corresponds to the source agent that sent the packet, the tunnel being configured by said source agent in accordance with a network protocol;
>
> ***making a routing decision for an authenticated packet at least in part without regard to contents of a payload of the packet, the routing decision being constrained based on the security association of the authenticated packet***;
>
> selecting a routing destination for a packet based at least partially on the routing decision; and
>
> routing the authenticated packet to the selected routing destination.

As is described above in relation to claim 1, Strahm's CFE does not, as is suggested in the Office Action, control routing based on a security association and without regard to contents of a payload of the packet. It logically follows that Strahm's CFE does not make "a routing decision for an authenticated packet at least in part without regard to contents of a payload of the packet, the routing decision being constrained based on the security

association of the authenticated packet". Claims 15-23 are allowable over Strahm for at least this reason.

3. Claims 24-25

Applicant's claim 24 provides as follows (emphasis added):

> 24. A computer program for performing network routing in accordance with a private network security technique, the computer program being embodied on a computer readable medium, the computer program comprising:
>
> a first code segment, the first code segment authenticating received packets sent from a source agent to a tunnel endpoint to determine whether a security association of a received packet corresponds to the source agent that sent the packet, the tunnel being configured by said source in accordance with a network protocol;
>
> a second code segment, the second code segment ***making a routing decision for an authenticated packet at least in part without regard to contents of a payload of the packet, the routing decision being constrained based on the security association of the authenticated***; and
>
> a third code segment, the third code segment selecting a routing destination for the authenticated packet based at least partially on the routing decision made by the second code segment.

As is described above in relation to claim 1, Strahm's CFE does not, as is suggested in the Office Action, control routing based on a security association. It logically follows that Strahm's CFE does not include a code segment that makes "a routing decision for an authenticated packet at least in part without regard to contents of a payload of the packet,

the routing decision being constrained based on the security association of the authenticated". Claims 24 and 25 are allowable over Strahm for at least this reason.

C. Conclusion

Due to the shortcomings of the Strahm reference described in the foregoing, Applicant respectfully asserts that Strahm does not anticipate Applicant's claims. Therefore, Applicant respectfully requests that the rejection of these claims be withdrawn.

III. Canceled Claims

Claim 13 has been canceled from the application without prejudice, waiver, or disclaimer. Applicant reserves the right to present this canceled claim, or variants thereof, in continuing applications to be filed subsequently.

CONCLUSION

Applicant respectfully submits that Applicant's pending claims are in condition for allowance. Favorable reconsideration and allowance of the present application and all pending claims are hereby courteously requested. If, in the opinion of the Examiner, a telephonic conference would expedite the examination of this matter, the Examiner is invited to call the undersigned attorney at (770) 933-9500.

Respectfully submitted,

David R. Risley
Registration No. 39,345

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail, postage prepaid, in an envelope addressed to: Assistant Commissioner for Patents, Alexandria, Virginia 22313-1450, on

1-12-06

Mary Meza

Signature